A View of BitLocker in Windows Vista Beta 2

By Aaron Powell and Christopher Vincent

Introduction

Overview

BitLocker is a technology designed to protect the data stored on a computer through "full volume encryption" and "secure startup." It is included in two editions of Windows Vista (Ultimate and Enterprise editions). Unlike encrypted file systems or file-specific encryption, full volume encryption protects an entire partition including the empty space and system files within the encrypted partition. Its goal is to prevent the unwanted recovery of data from a stolen or discarded hard drive.

In addition, BitLocker can utilize a machine's Trusted Platform Module (TPM), if present, to control key access and prevent unauthorized access of a secure volume.

What is Secure Startup?

BitLocker can perform both hardware authentication and user authentication at startup to ensure that the hardware and/or user accessing the Windows Operating System have the authority to do so. In other words, BitLocker prevents the Operating System from booting and decrypting the drive until the user presents some combination of something they have (a USB key or the machine's TPM) and/or something they know (PIN or recovery password).

How is Secure Startup Different from Full Volume Encryption?

Secure Startup protects the keys needed to decrypt and access the Windows volume, whereas full volume encryption protects the data. BitLocker uses both by default, but Secure Startup can be disabled via the BitLocker control panel by choosing to "turn off" BitLocker without decrypting the Windows volume. Note that with BitLocker off and the volume encrypted there is no barrier to data access beyond a user's (often weak) login credentials.

What problems might I face when using the TPM?

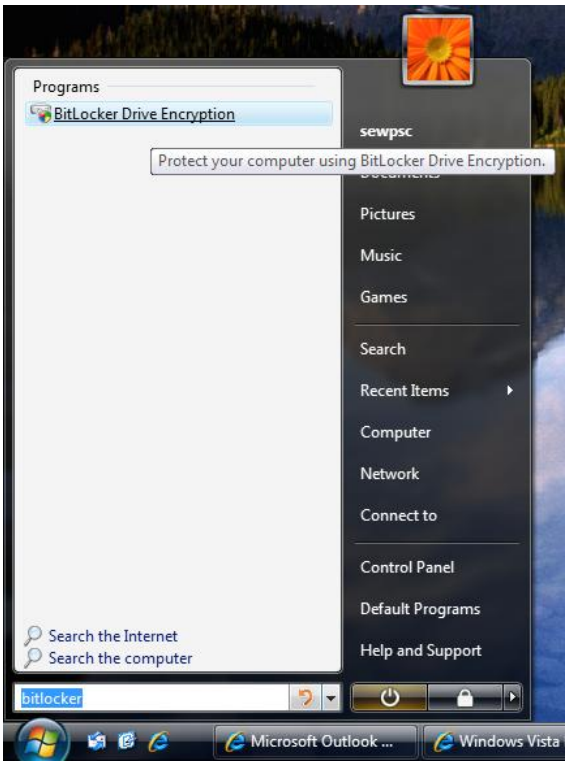
BitLocker's ability to use Trusted Platform Module (TPM) hardware gives it a high level of security by cryptographically binding the Windows volume to the physical machine in which it resides. This prevents an attacker from accessing the data after removing a hard drive from a machine. Despite our Dell OptiPlex GX620's inclusion of a version 1.2 TPM chip (version 1.2 is required by BitLocker), Windows

Vista Beta 2's TPM Services could not recognize the hardware due to the lack of proper BIOS support from Dell. Thus we were unable to test BitLocker's TPM-enabled features.

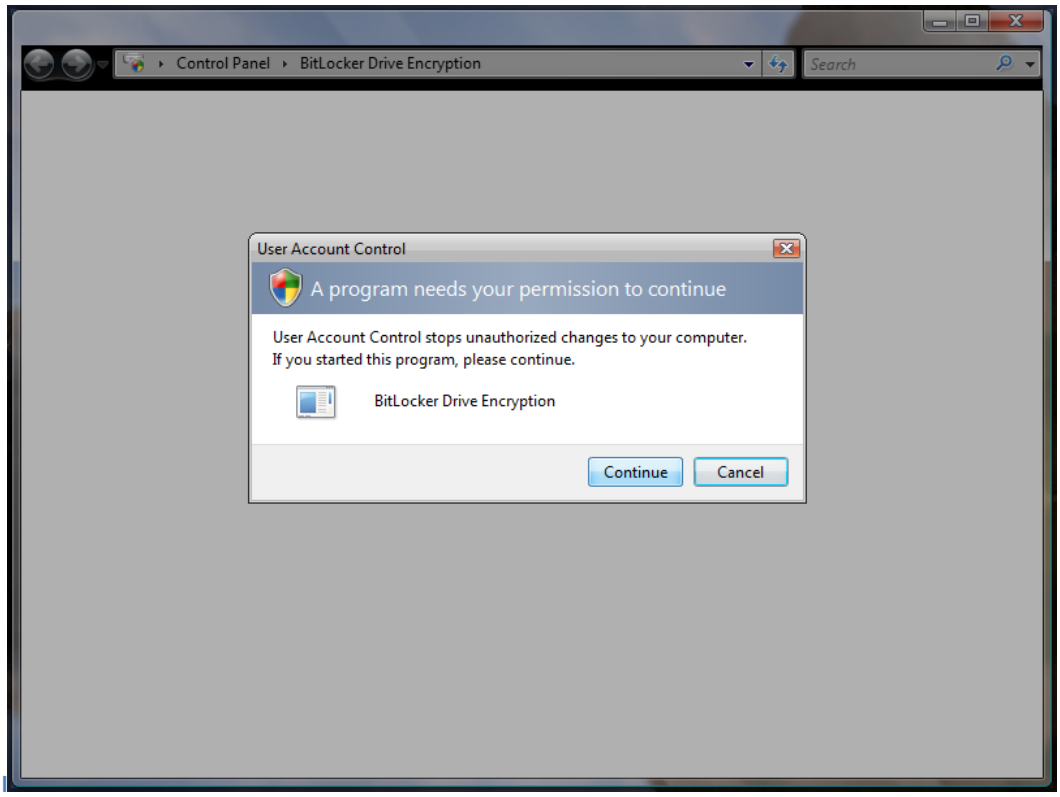
Although many manufacturers advertise TPM-capable machines, support for such hardware does not appear to be available for Vista, especially from Dell.

Setting up BitLocker

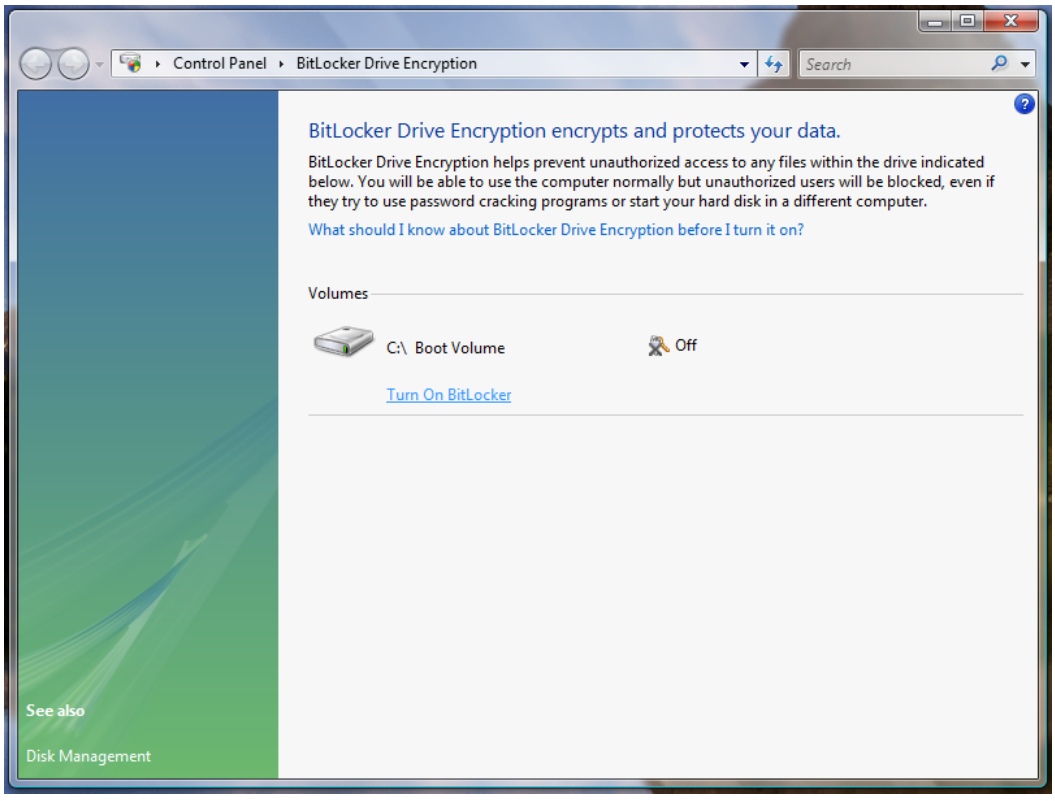
The following steps depict the process of enabling BitLocker in a Secure Startup using USB key only mode.



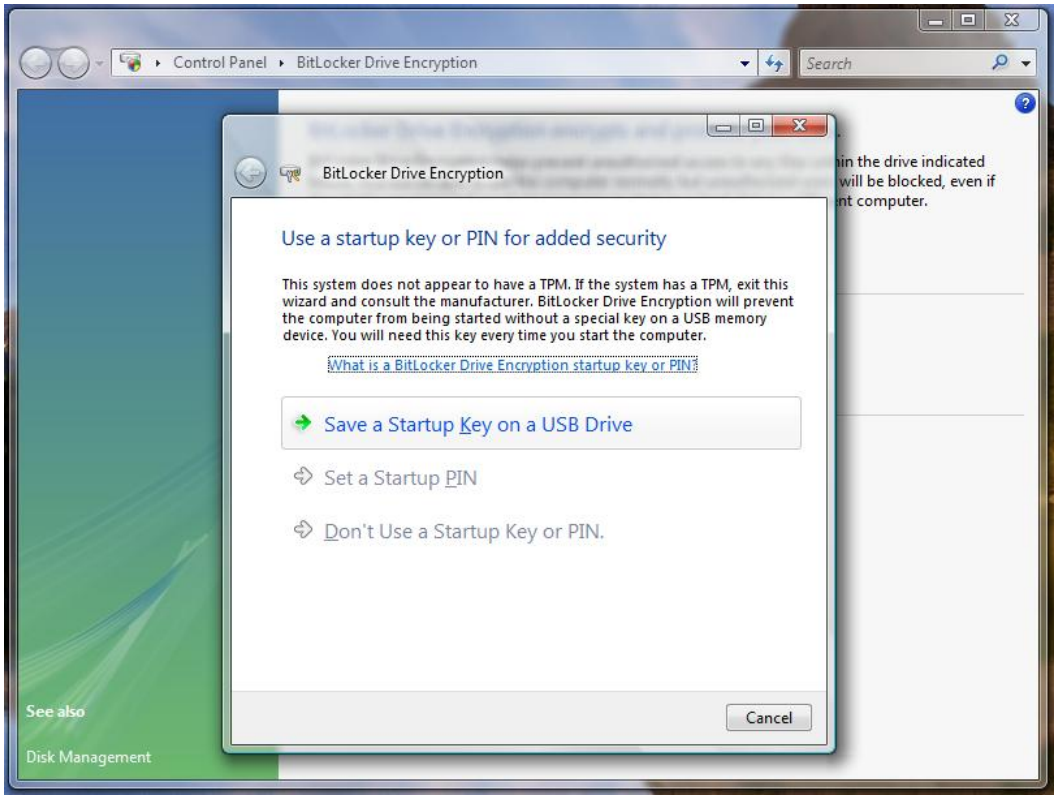
Step 1: Open BitLocker control panel via Start Menu search



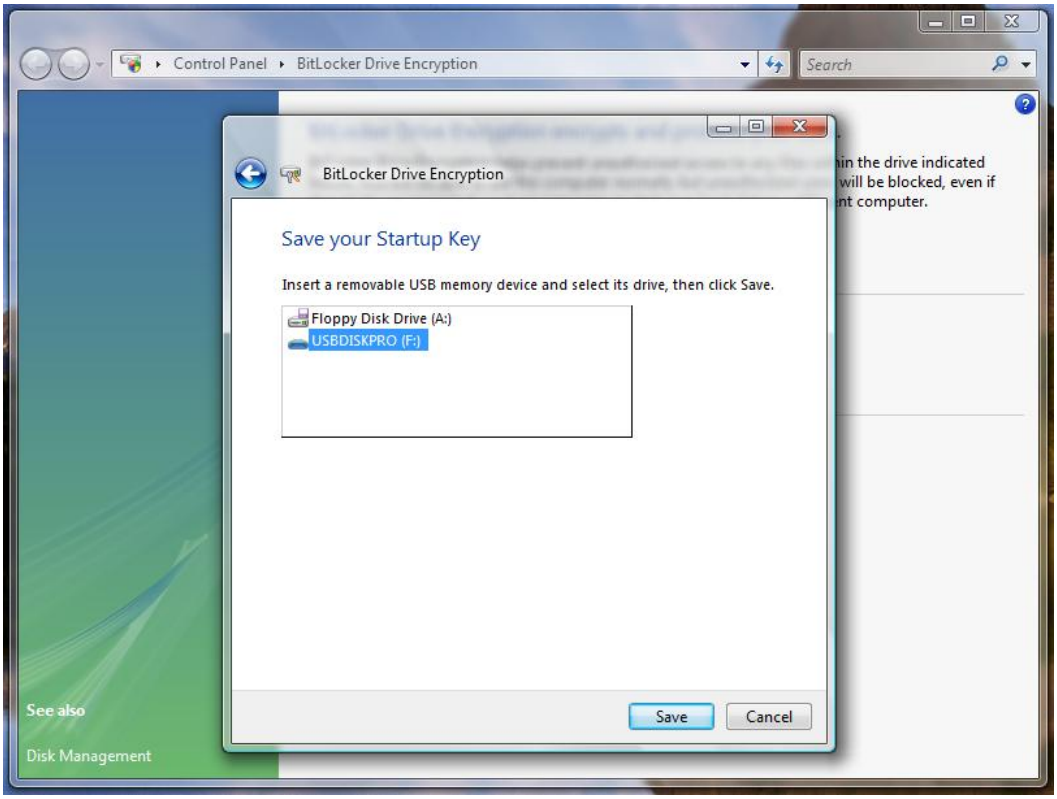
Step 2: Click “Continue” to give permission to open the BitLocker control panel



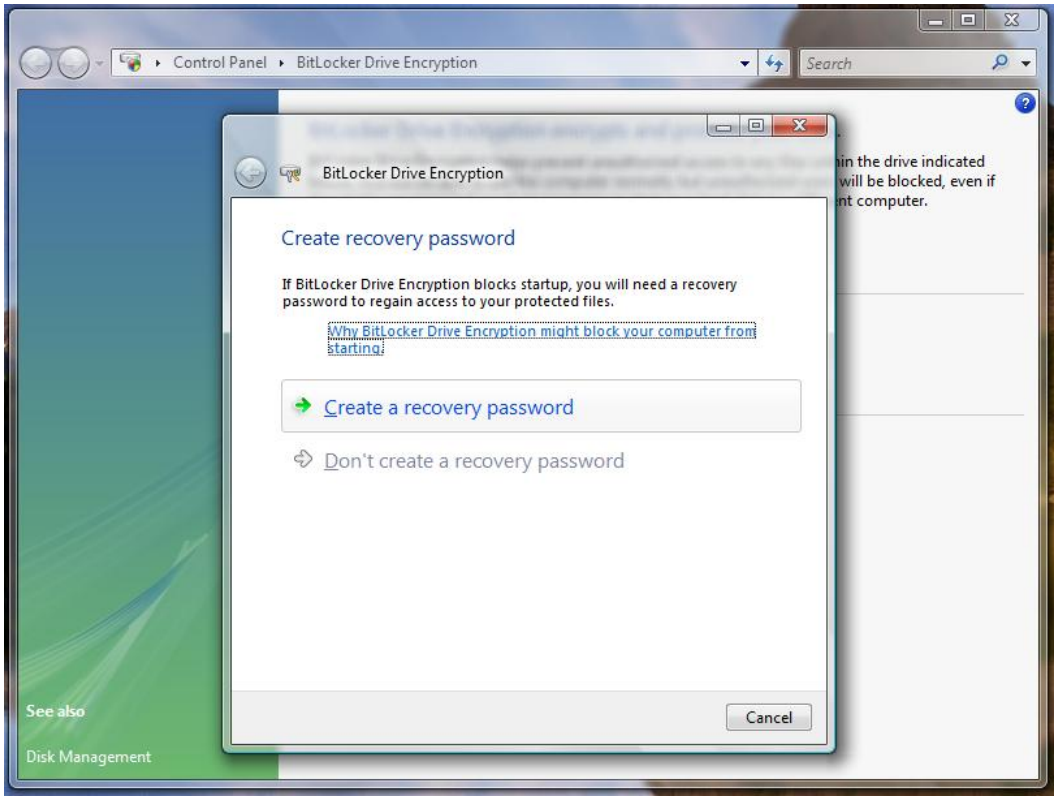
Step 3: Click on "Turn On BitLocker"



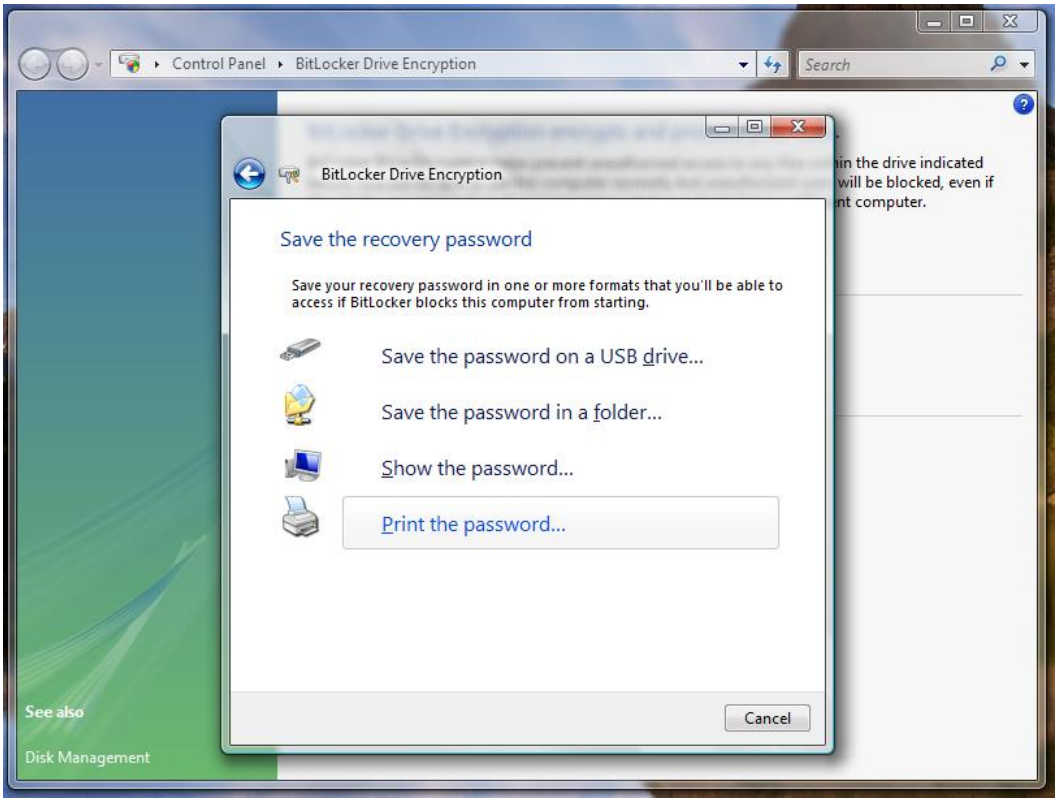
Step 4: Click on "Save a Startup Key on a USB Drive"



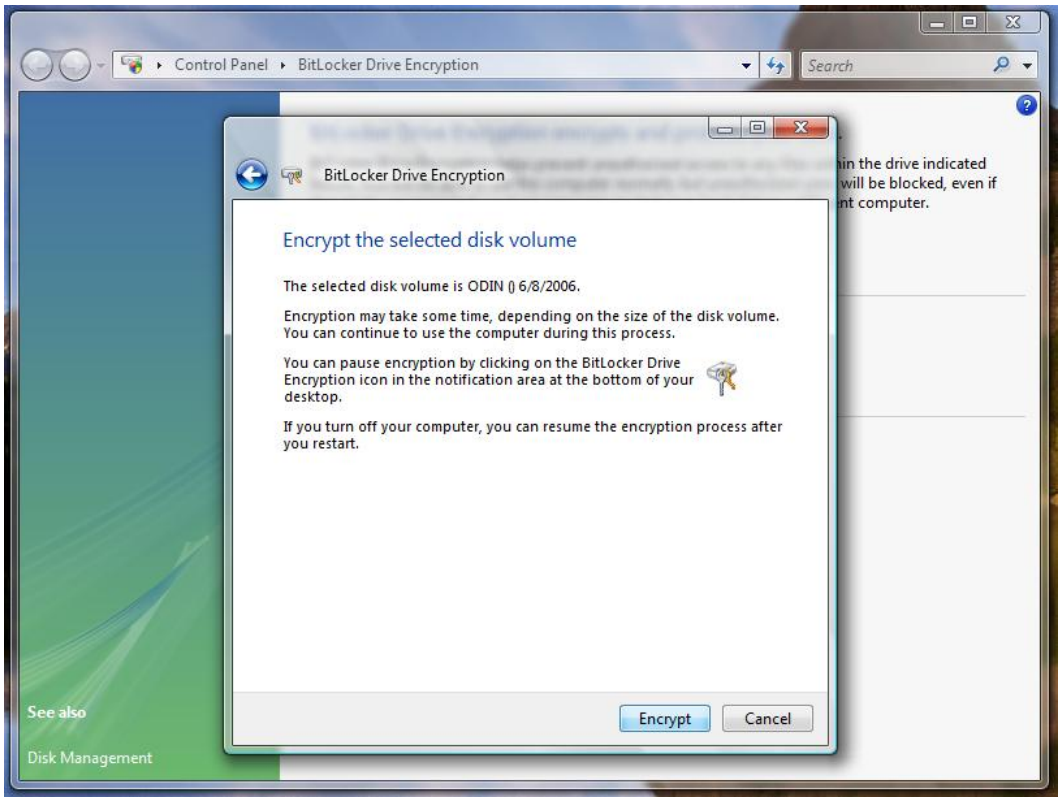
Step 5: Choose a USB drive on which to store the secure startup key and click "Save"



Step 6: Click on "Create a recovery password"



Step 7: Safely store the recovery password (we recommend choosing "Print the password...")



Step 8: Click on "Encrypt" to start encrypting the Windows volume

This concludes the setup process. The setup process for other BitLocker "modes" is similar, and guides to BitLocker setup (*as defined in Beta 2 of Vista*) can be found in the "Additional Resources" section of this document.

Security Concerns

Hibernation and Sleep

In addition to or in lieu of TPM-based authentication, an administrator can configure BitLocker to requirethe user to insert a USB key at boot time. Windows also has a feature called "Hibernate" in which the contents of the PC's RAM are written to the hard drive, unlike "Sleep" where the contents of the PC's RAM stay intact. Windows treats "Hibernate" in almost exactly the same way as it treats the normal boot process, so BitLocker requires the (re)insertion of the USB key when waking from "Hibernate." On the other hand, the normal "Sleep" does not require the insertion of the USB key, so administrators should take care to configure machines with a set of policies that match the organization's needs. An administrator can reduce the risk of circumvention of BitLocker (through theft of a "sleeping" rather than "hibernating" machine) by reducing the duration before the machine goes into "Hibernation." Administrators ought to be wary, though, because too frequent hibernation might induce PC users into leaving the USB key plugged into the machine at all times thus rendering the USB key irrelevant.

Fault Tolerance

Limited experimentation has revealed to us that BitLocker probably encrypts individual sectors on the disk independently. Thus, an error in the recording of a single byte to the hard drive or a modification of the state of a single byte on the hard drive will probably corrupt the entire sector (e.g. 512 bytes) due to failed decryption. NTFS seems to have an array of features to protect against damaged hard drive data, but a loss of 512 bytes would exceed the typical loss on an unencrypted system. As a result, BitLocker encrypted drives will probably suffer slightly higher rates of data loss, as compared with unencrypted systems.

Root Kits

At the present time, kernel-space root kits are guarded against in 64-bit versions of Vista. The effectiveness of these guards is currently unknown to the Security Center, and it is important to note that for compatibility reasons Microsoft has decided not to include such guards in its 32-bit versions of Vista.

Performance Considerations

The following results were attained running 64-bit Windows Vista Ultimate Edition Beta 2 on a Dell OptiPlex GX620 with 1GB RAM and a 3.2 GHz Pentium 4 with HyperThreading enabled.

Setup

During initial volume encryption, the processor load sustained around 50% and hard drive throughput spiked between 0 and 60 MBytes/sec. Due to the symmetric nature of the AES encryption employed by BitLocker, decryption should exhibit similar results. In addition, the “Properties” panel of the encrypting drive showed 99% usage (with only 1GBytes of free space available) during the encryption process, limiting the capacity of a user to perform certain hard-drive-space-intensive tasks.

Normal Usage

BitLocker has a definite impact on computation and storage throughput. Normal users should not notice any large impact, but any application that is disk or computation-intensive may be considerably slower. Without BitLocker enabled, a file duplication task attained throughput of ~29 MBytes/sec sustained, whereas with BitLocker disabled the throughput was significantly less at ~18 MByte/sec. Processor load during the file copy was ~15% with BitLocker off and ~%50 with BitLocker on.

Other Considerations

Drive Sanitization

As recently as May of 2006, advocates of Microsoft’s BitLocker feature have suggested that BitLocker provides an alternate method of data destruction, or disk sanitization. The claim is that by destroying all the primary and recovery keys (via clearing the TPM, securely erasing any keys stored on removable

media, and shredding any hard copies of recovery keys), system administrators can more efficiently render data permanently inaccessible. Currently, disk sanitization is a time-intensive (and therefore costly) process, and use of BitLocker offers the potential to reduce this cost. However, system administrators must be particularly careful when relying on BitLocker for disk sanitization due to the potential propagation of key information through escrow, backup, and other automated systems. Merely erasing a recovery key and clearing the TPM may not provide reliable sanitization in a complicated environment. Further, it is currently unclear whether encryption-based sanitization is sufficient to meet contractual or statutory obligations for data destruction.

Drive Backup & Restoration

As a result of BitLocker's full volume encryption, software designed to create backup and restoration points from outside the Operating System (for instance, Symantec Ghost) will require significantly more storage space and network transmission if applicable. The fact that the volume is encrypted prevents any software external to the OS from reading any of the file system's contents; thus, efficient and quick differential backups or drive images that typically exclude free space are not feasible. Environments requiring large-scale backup and restoration of remote machines should consider the effect BitLocker may have on a given network or machine resource. Future backup solutions would need to be BitLocker-aware to perform such tasks successfully.

Disabling BitLocker: Turning Off Secure Startup v. Decrypting the Volume

Merely disabling BitLocker via the "Disable BitLocker Drive Encryption" option seems to disable only the secure startup mechanism and not the encryption of files on disk. To turn it off completely and ensure one's Windows volume is fully decrypted, the "Decrypt the volume" option must be chosen. Please refer to the figure below.

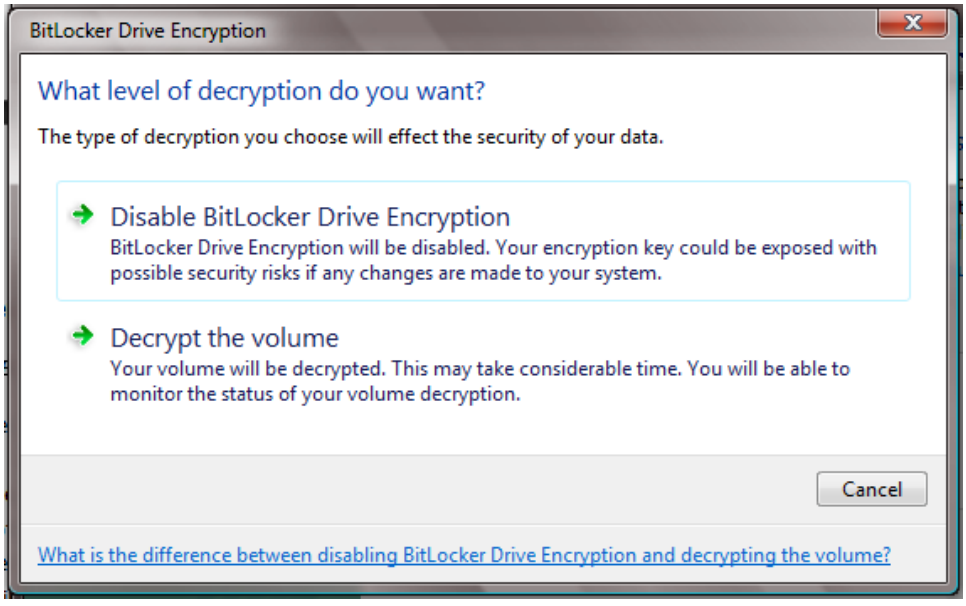


Figure 1: Options when Disabling BitLocker

Additional Resources

Windows Vista Beta 2 BitLocker Drive Encryption Step-by-Step Guide.
http://www.microsoft.com/technet/windowsvista/library/c61f2a12-8ae6-4957-b031-97b4d762cf31.mspx

Windows Vista Beta 2 Trusted Platform Module Services Step by Step Guide.
http://www.microsoft.com/technet/windowsvista/library/29201194-5e2b-46d0-9c77-d17c25c56af3.mspx

Exclusive: Q&A with the Windows Vista BitLocker Team.
http://windowsconnected.com/blogs/joshs_blog/archive/2006/03/03/1144.aspx

Schneier on Security: Microsoft's BitLocker.
http://www.schneier.com/blog/archives/2006/05/bitlocker.html